Maryland Third Party Interconnection Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority. This includes ensuring that acceptable security measures are in place, and that acceptable risk levels are maintained, when new network connections are made between Maryland agencies and **third party** entities.

This policy outlines the requirements of secure third party interconnections. DoIT will utilize the baseline controls and standards established by NIST SP 800-53R4 and 800-47 to develop **Third Party Interconnection** requirements.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013), Section 5.3: Service Interface Agreements and any related policy regarding third party interconnection declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all IT environments and assets utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology. DoIT will be responsible for ensuring the security of third party connections in accordance with the requirements in this policy for all agencies within the DoIT Enterprise environment.

Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy.

4.0 Policy

The requirements governing secure third-party connections are listed in the table below.

#	Name	Requirement
A	Planning	Third party interconnections will be planned in advance. Planning will be conducted in accordance with industry best practice as noted in NIST SP 800-47 “Security Guide for Interconnecting Information Technology Systems”.
B	Security Assessments	Third party interconnections must provide a **Systems Security Plan (SSP)** to the agency’s Designated Approval Authority (DAA) for a security review. This person may be the: ▪ Agency’s Deputy CIO; or ▪ Director of Cybersecurity/State CISO or designated official (if agency IT or security decisions are handled by DoIT)

#	Name	Requirement
C	Compliance with DoIT Cybersecurity Policies	▪ Insofar as the third party has connectivity to agency systems or networks, or access to agency data, the third party will comply with all applicable DoIT Cybersecurity Policies. ▪ The third party must inform the DAA of any change to its infrastructure affecting the interconnection.
D	Confidentiality and Non-Disclosure	Insofar as any data, systems, or networks to which the third party has access are considered confidential to the agency, the third party must sign Confidentiality and Non-Disclosure Agreements (NDA).
E	Technical Documentation of Connection	Technical details regarding the third party interconnections will be documented; this shall include, at a minimum: ▪ Description of the purpose of the connection; ▪ Updates to agency logical and physical topology diagrams to account for the connection (or a supplementary diagram); ▪ Allowed protocols; ▪ Allowed network addresses or address ranges; ▪ Allowed TCP/UDP ports if applicable; ▪ Allowed data types; and ▪ Authorized users (with specific names or user groups)
F	Monitoring Activation	Third party interconnections shall not be authorized until security monitoring of that connection has been enabled in accordance with the DoIT *Continuous Monitoring Policy*.
G	Least Privilege	New third party interconnections will: ▪ Grant the minimum connectivity into the agency required to meet the objectives of the connection ▪ Grant the minimum access privilege required to meet the objectives of the connection
H	No Full Network Access	Unfiltered network connections (WAN, LAN, WLAN, VPN, etc.) between the agency and any third parties other than DoIT itself, will not be authorized or allowed. NOTE: Connectivity to an agency LAN by a third party-owned or supplied computer system constitutes FULL NETWORK ACCESS without compensating controls, and thus is disallowed by default. Alternatives to connecting to an agency LAN include: ▪ Provisioning a guest network for third party Internet access from an agency facility ▪ Provisioning agency-owned workstations for use by third party staff who require access to agency systems. EXCEPTION: Vendors providing penetration testing services may be granted additional elevated privileges under the conditions established within the scope of the evaluation.
I	Third Party Contact Information	▪ The third party will be required to provide contact information to the agency for the appropriate groups or individuals who can fulfill agency requests for cyber security monitoring and incident handling ▪ Contact information will include emergency contact information for off-hours requests ▪ The agency will maintain this contact information so that it is immediately accessible to IT and IT security staff as needed

#	Name	Requirement
J	ATO or IATO	In order to be activated, all third party interconnections require an Authority to Operate or Interim Authority to Operate signed by the agency's Designated Approval Authority (DAA) for security matters.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Boundary Protection and Internet Access Policy
- Continuous Monitoring Policy
- Cybersecurity Authority to Operate
- Security Assessment Policy

7.0 Definitions

Term	Definition
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Third Party	Any entity or computing environment that is not the Maryland agency complying with this policy.
Third Party Interconnection	Any IT connection to a third party that enables the transfer of data between the agency and the third party, or the sharing of computing resources. This includes, but is not limited to: ▪ Direct network connection (Local Area Network, Wide Area Network, etc.); ▪ Virtual Private Network (VPN) connection; ▪ Shared computing platforms. For example, an agency virtual machine hosted on a server or cluster that also hosts non-agency virtual machines would constitute a third party connection; or ▪ Known usage of external storage media to move data between the agency and the third party.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for ensuring the security of third party connections for Enterprise onboarded agencies. The DoIT Cybersecurity Program identifies the minimum requirements necessary to comply with the information security standards and guidelines provided within Cyber Security Program Policy and its supporting

policies. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies.

If DoIT determines that an agency is not compliant with this policy or any supporting policy, the non-compliant agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize a DoIT representative to limit or restrict an agency's access to external and internal communications (effectively shutting down connectivity) until such time the agency becomes compliant.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.